Google Scholar BETA

Web Images Video News Maps more »

"quick mode" "main mode" IKE nonce Search

Advanced Scholar Search
Scholar Preferences
Scholar Help

Scholar All articles - Recent articles Results 1 - 10 of about 159 for "quick mode" "main mode" IKE nonce. (0.35 s

Fixing of security flaw in IKE protocols
J Zhou - Electronics Letters, 1999 - ieeexplore.ieee.org
... basic modes: main mode and aggressive mode, used in phase 1, and quick mode, used in ... There are six rounds of exchanges in the main mode protocol. ... IKE message. ...
Cited by 39 - Related articles - Web Search - BL Direct - All 4 versions

Further analysis of the Internet key exchange protocol - [PDF] ▶ a-star.edu.sg
J Zhou - Computer Communications, 2000 - Elsevier
... its security association payload in the quick mode protocol ... In Phase 1 of the IKE protocol, the initiator and ... Here we use the main mode protocol with pre-shared ...
Cited by 48 - Related articles - Web Search - All 11 versions

Methods and protocols for secure key negotiation using IKE
MS Borella - Network, IEEE, 2000 - ieeexplore.ieee.org
... Secure Key Negotiation Using IKE ... cols of IPsec's Internet Key Exchange and discuss the types of security that the various IKE modes provide. ...
Cited by 30 - Related articles - Web Search - BL Direct - All 3 versions

IKE/ISAKMP Considered Harmful - [HTML] ▶ tu-chemnitz.de
WA Simpson - USENIX; login, 1999 - usenix.org
... One common IKE/ISAKMP implementation used over 50MB of memory during a ... Although the "Quick" mode relies on the security of the "Main" mode of operation ...
Cited by 11 - Related articles - Web Search - All 3 versions

Analysis of the Internet Key Exchange protocol using the NRLProtocol Analyzer
C Meadows - Security and Privacy, 1999. Proceedings of the 1999 IEEE ..., 1999 - ieeexplore.ieee.org
... init keymain subprotocol corresponding to main mode , or the ... such as including identities in Quick Mode messages are ... to a protocol suite like IKE, it became ...
Cited by 124 - Related articles - Web Search - Library Search - BL Direct - All 10 versions

Efficient, DoS-resistant, secure key exchange for internet protocols - [PDF] ▶ cryptо.com
W Aiello, SM Bellovin, M Blaze, J Ioannidis, O ... - Proceedings of the 9th ACM conference on Computer and ..., 2002 - portal.acm.org
... But our motivation is especially colored by our experience with IKE. ... mod p). g r Responder's current exponential, (mod p). N I Initiator nonce, a random bit ...
Cited by 82 - Related articles - Web Search - BL Direct - All 33 versions

[CITATION] Performance evaluation of the Internet Key Exchange Protocol under dynamic VoIP network conditions
B Springer, L Kilmartin - Proceedings ISSC 2003
Cited by 3 - Related articles - Web Search

[PDF] ▶ Using the NRL Protocol Analyzer to examine protocol suites
C Meadows - LICS Workshop on Formal Methods and Security Protocols, 1998 - people.emich.edu
... Quick mode uses Die-Hellman key exchange, and can be used ... 5 Current State of the Analysis of the IKE Protocol ... to do either, but in the case of main mode with ...
Cited by 9 - Related articles - View as HTML - Web Search - All 3 versions

[TXT] ▶ An architecture for the Internet Key Exchange Protocol
PC Cheng - IBM Systems Journal, 2001 - research.ibm.com
... a passive adversary can decipher all QUICK mode negotiations protected ... because IKE Phase I has a main mode and an ... initiator and the responder of an IKE Phase I ...
Cited by 18 - Related articles - Cached - Web Search - BL Direct - All 10 versions

IPsec Networking Standards—An Overview
N Dunbar - Information Security Technical Report, 2001 - Elsevier
... is still an expensive operation, and so Quick Mode exchanges do ... Only Main Mode is required to be implemented for IKE. ... on both sides of the IKE exchange, the ...
Cited by 9 - Related articles - Web Search - All 2 versions

Key authors: J Zhou - W Aiello - C Meadows - N Ferguson - S Bellovin

Gooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 Next

"quick mode" "main mode" IKE nonc Search

Google Home - About Google - About Google Scholar